

Frameo Privacy Policy

Frameo A/S (“Company” or “frameo” or “we” or “us” or “our”) operates <https://frameo.net/> and <https://frameo.com/> (the “site”) and provides the frameo mobile app for Android and iOS (the “app”) and the frameo frame app (the “frame”).

We take your privacy seriously and are committed to protecting the information we collect. We have written our privacy policy to be understandable for humans (not just lawyers). By using our app or frame, future products, services or features we develop and introduce, or our website (together the “Services”), you consent to the collection, processing and disclosure of data concerning you in accordance with this Privacy Policy.

You may find our [Terms of Service here](#).

Data collection

Information we collect when you use our Services:

Log Data - to ensure that our Services are performing optimally.

We collect some of the information generated by our services (“Log Data”). This Log Data may include information such as your device’s Internet Protocol (“IP”) address, browser type, browser version, the pages of our site that you visit, the time and date of your visit or use of the app or frame, the time spent on those pages, which IPs communicate together through our servers and other statistics. IP addresses are anonymized wherever possible. Log Data is collecting from all Services, including the frame and the app.

Specifically for photos and videos shared through the app we collect only information about the transfer status and metadata about the media (eg. the resolution of a photo).

Communication between app and frame is end-to-end encrypted which makes it impossible for us or any third party to see your photos or videos.

This ensures your privacy when using our Services.

Behaviour Data - to ensure the optimal user experience.

Cookies and Similar Technologies:

We may collect information about your use of our Services through the use of cookies, pixels or similar technologies. For example, we may use this information to provide or improve our Services, for measurement and analytics to better understand how our Services function and are used, or for internal operations. Cookies are small pieces of data that are stored on your mobile phone, computer, or other device. Pixels, often used in connection with cookies, are

small instances of code placed in web pages that do things like allow another server to measure how frequently web pages are viewed and used.

Third parties may also use cookies to collect information about your activities on our website. Your browser or device may offer you control over the use of cookies or other technologies when you use the Services. For example, you may be able to set your browser or device to disable, clear, reset or block the use of cookies or similar technologies.

Personal information we collect when you create a Regular Account:

When you create a Regular Account in your Frameo app you may provide us with the following data: Name and Email address. No other personal information is collected from the creation of the user account.

Personal information we collect when you add a subscription to your Regular Account:

None.

The payment is handled by Google Payments or Apple Pay, so there is no need for Frameo to collect any personal information. Furthermore, information regarding your payment, such as credit card information, is not shared with Frameo by Google Payments or Apple Pay.

Third Party Data Processing

We use automated devices and applications to evaluate usage of our app, frame and site. We also may use other analytics to evaluate our Services. We use these tools to help us improve our Services, performance and user experience. We do not share your personal information with these providers if not strictly necessary to evaluate and optimize your experience. Some of our providers of these devices and applications are either located or have parent companies in the US. Where this is the case, our providers are certified under the EU-U.S. Data Protection Framework and all data transfer is protected with the necessary safeguards in accordance with GDPR art. 45.

For providers located outside of the EU who are not DPF certified, data processing agreements in accordance with the EU standard contractual clauses have been entered providing the necessary safeguards in accordance with the GDPR art. 46. If you wish to receive a copy hereof, you are welcome to contact us.

Joint controllership:

Frameo may from time to time use pixel technology such as Facebook Pixel, LinkedIn insight Tag and Google analytics. These tools allow us to measure and optimise our website and ads to make them more relevant to you. The collected data remains anonymous to Frameo since we cannot identify you from this data. However, the data may be saved and processed by Facebook, LinkedIn and Google for their own advertising purposes and they may in some

cases be able to identify you by combining the data with data about you that they have previously obtained. It is Facebook, LinkedIn and Google who has the ultimate control of the information gathered through the mentioned pixel technology. You can opt-out of these technologies by declining tracking and performance cookies as well as targeting and advertising cookies on our website.

Legal basis for processing personal data

When we process your personal data, we always ensure that the processing is in accordance with the GDPR and other relevant legislation, namely that we always have a legal basis for the processing.

The legal basis for our processing of analytic data from cookies on our website is the GDPR art. 6(1)(a) and the Danish Executive Order on cookies section 3.

The legal basis for our processing of analytic data from our website and app, that is not derived from the use of cookies, is the GDPR Art. 6 (1)(f), as it is in our legitimate interest to make our Services available to you, including improving and optimising the user experience.

Lastly the processing of contact information such as name and e-mail address are processed based on the GDPR art. 6(1)(f) as it is in our legitimate interest to be able to contact our customers. Where we use your contact information to send newsletters and other marketing material, this is based on GDPR Art. 6(1)(b) as the processing is necessary in order to send you the newsletters if agreed by you.

Your rights as data subject

You have the rights as described below which you can exercise by contacting us at the below mentioned contact information. Your request will be answered free of charge, as soon as possible and no later than one month after receipt, however, up to two months if necessary due to the complexity or number of requests. In the event of unfounded or excessive requests, we have the right to reject it or charge a reasonable fee for answering it.

Your specific possibilities are:

- **Withdraw consent**

To the extent processing is based on your consent, you may at any time withdraw your consent by contacting us at the below mentioned information or as otherwise explained when you provided your consent. This will not affect the lawfulness of the processing before its withdrawal.

- **Access**

You have the right to access the personal data that we process about you, as well as

certain information about how the processing takes place. No access is granted to information which must remain confidential because of public or private interests, including your own interests.

- **Rectification**

You have the right to have incorrect personal data corrected or to have incomplete personal data about you completed.

- **Erasure**

You have the right to have personal data about you deleted in the circumstances specified in Article 17 of the GDPR. This may be the case, for example, if the information is no longer necessary for the fulfilment of our obligations and exercising of our rights or if the information is processed on the basis of your consent which has been withdrawn.

- **Restriction**

In the circumstances mentioned in Article 18 of the GDPR, you have the right to have the processing of your personal data restricted, e.g. if the accuracy of the data is disputed, in the period until we have had the opportunity to determine whether the personal data is correct or if we no longer need the personal data for the processing but they are necessary to establish, exercise or defend a legal claim.

- **Object**

You have the right to object to the processing of personal data which we process on the basis of Article 6(1)(f) of the GDPR (the legal basis for processing in our legitimate interest) and always if the processing is for the purpose of direct marketing.

- **Data portability**

If the processing is based on your consent or contract, you have the right to receive the information in a plain and readable format and to transmit the information to another data controller. If you wish and if technically possible, we will transmit the information directly to this data controller.

- **Automatic decisions**

You have the right not to be the subject of an automatic decision that has legal effect or similarly significantly affects you, which is based solely on automatic processing, including profiling.

Deletion of data

Information required for newsletters is kept until the consent is withdrawn or the consent has not been used for one consecutive year. We keep documentation that you have withdrawn your consent for up to 2 years after the consent has been withdrawn, in order to be able to

defend us against any claims made for violation of the Danish Marketing Act, cf. § 37, subsection 3 and the Danish Penal Code § 93, subsection 1, no. 1, however only if there is an actual risk that such a claim will be made.

Personal data contained in cookies is deleted when the cookie expires or is deleted by you. Other analytics data such as IP-addresses are deleted after 13 months.

Your personal data is kept until you choose to disable your Regular Account. In that case profile data including online backup of your frames is kept for 2 months for the purpose of recreating the Regular Account if you should change your mind. After 2 months all personal data about you will be automatically deleted.

Security

We take security of your information seriously and use reasonable electronic, personnel, and physical measures to protect it from loss, theft, alteration, or misuse. However, please be advised that even the best security measures cannot fully eliminate all risks. We cannot guarantee that only authorised persons will view your information. We are not responsible for third party circumvention of any privacy settings or security measures. Also note that since frames are designed exclusively for home use, the media presented on them is not hidden behind a password screen and can therefore be physically accessed by anyone in the home.

Changes to our privacy policy

We reserve the right to alter our privacy policy at any time. We will notify you of any alterations with reasonable notice through the service, such as by posting it on our website, by email, or otherwise. If you do not agree to the altered privacy policy, you may stop using our Services.

Contact

Should you wish to exercise any of your rights or if you have any questions regarding our Privacy Policy, please contact us via email: contact@frameo.net

EU Data Act compliance

This section specifically describes Frameo's compliance with the EU Data Act. As this legislation is brand new it is expected that this section will be updated over time as it becomes more clear how best to communicate this compliance or how to incorporate it with the rest of our data handling descriptions.

Data overview

The type, format and estimated volume of product data

The data described below is generated across the Frameo services (i.e. the Frameo Frame app on the digital photo frame, the Frameo app on either Android or iOS, and the connected online services enabling the usage of the Frameo software product).

Frameo uses system information and usage data to guide development. That encompasses the process for improving the existing functionality, finding and fixing bugs and developing new features.

Application data

This data is core to the function of the frame. It contains the user content uploaded to the frame, feature data (e.g. reactions, weather data, etc.), information about connected frames and data related to app settings.

Format of data

Data consists of structured data in XML and binary data that can be parsed as databases.

Volume of data

Will depend mainly on the amount of content shared to the frame. The data may be compressed to reduce the amount of storage used.

As a general guideline here are some example sizes:

- Photo file sizes
 - Example: One Frameo photo on a 1920×1080 screen is ~ 1.3 MB
 - Example: One Frameo photo on a 1280×800 screen is ~ 0.8 MB
- Video file size
 - Example: One Frameo video sent to a 1280×800 screen is from 1 MB to 10 MB when the video duration is from 3 sec to 15 sec

Lifetime of data

Local data lives until it is manually deleted on the device or the app is cleared.

Data storage location

Stored locally on the device, phone or frame.

System Information

This includes information about the hardware and software platform that the software is running on, information regarding production, unique device identifiers as well as resource metrics like available disk space, memory and uptime.

Format of data

Data consists of structured data in XML, comma separated text files and other readable structured text saved to files.

Volume of data

The storage footprint of system information is very small, less than a MB per day.

Data storage location

Most system information is stored locally. System information and metrics are briefly stored locally before being uploaded securely and stored on remote servers.

Lifetime of data

System identifiers data saved on the device persist across factory reset. Data which is anonymized and cannot be linked to an individual user, may be kept for longer periods for statistical purposes.

Usage data

Information is collected about how the product is used. This data is encapsulated as events that details how features and functionality of the frame have been used.

Format of data

The raw data is temporarily stored in a proprietary binary format on the device. It is then uploaded and stored remotely in a structured, event-based format.

Volume of data

The volume of data will depend on the usage of the Frameo services, in particular how much interaction is made with the apps. Most significant interactions with the apps will result in one or more generated events.

Data storage location

The data is briefly stored locally before being uploaded securely and stored on remote servers.

Lifetime of data

User-specific data is collected and kept until the user deletes their account. Data which is anonymized and cannot be linked to an individual user, may be kept for longer periods for statistical purposes.

Continuous and Real-Time Data Generation

The product is capable of generating data continuously (real-time) while it is powered on.

This data is sent to our servers in near real-time. This allows for immediate analysis of performance issues and timely updates to improve your experience.

How to Access, Retrieve, and Erase Your Data

Data stored on device

Accessing local data on the Frame can be done by using the built-in export feature, or through adb access. It is also possible to access a backup of the Frame content if one has been made: <https://support.frameo.com/hc/en-us/articles/360021672160--How-to-Make-a-Backup-of-a-Frame>

Accessing iOS app data can be done through standard iOS platform methods for accessing app data.

Accessing Android app data can be done through standard Android platform methods for accessing app data.

Clearing the data can be done by resetting the frame or clearing/uninstalling the phone app respectively.

Data stored remotely

Contact Frameo support by email to support@frameo.com for requests about retrieving your remotely stored data. Frameo is able to provide you with the data that has been stored on our servers on a per-request basis. Data will be made available to you via the mail that has been connected to your Frameo account.

Please see the section on “Deletion of data” for more information on deleting remotely stored data.

There are no additional charges for accessing, retrieving, or erasing your data. Data requests are typically processed within 30 days.

Last updated: 19-09-2025